नई राष्ट्रीय साइबर सुरक्षा रणनीति की ओर

चर्चा में क्यों?

28 अगस्त, 2019 को नई दिल्ली में 'नई राष्ट्रीय साइबर सुरक्षा रणनीति की ओर' (Towards New National Cyber Security Strategy) विषय पर 12वें भारतीय सुरक्षा सम्मेलन का आयोजन किया गया।

सम्मेलन के प्रमुख विषय

- सम्मेलन के दौरान महत्त्वपूर्ण राष्ट्रीय आधारभूत ढाँचों की सुरक्षा, उभरते साइबर खतरों, घटनाओं, चुनौतियों एवं प्रतिक्रिया जैसे कई विषयों पर चर्चा की गई।
- साथ ही इस विषय पर भी ध्यान केंद्रित किया गया कि 'डिजिटल संस्कृति' एक पीढ़ी से दूसरी पीढ़ी में परिवर्तित हो रही है। हर प्रौद्योगिकी की अपनी उपयोगिता है, इसी तरह साइबर प्रौद्योगिकी में इन दिनों बड़ी तेज़ी आई है। लेकिन एक वरदान होने के साथ ही यह प्रौद्योगिकी एक बड़ा खतरा भी बन गई है।

साइबर अपराध क्या है?

साइबर अपराध ऐसे गैर-कानूनी कार्य हैं जिनमें कंप्यूटर एवं इंटरनेट नेटवर्क का प्रयोग एक साधन अथवा लक्ष्य अथवा दोनों के रूप में किया जाता है। ऐसे अपराधों में हैकिंग, चाइल्ड पॉर्नोग्राफी, साइबर स्टॉकिंग, सॉफ्टवेयर पाइरेसी, क्रेडिट कार्ड फ्रॉड, फिशिंग आदि को शामिल किया जाता है।

साइबर अपराधों से निपटने की दिशा में भारत के प्रयास

- भारत में 'सूचना प्रौद्योगिकी अधिनियम, 2000' पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिये पर्याप्त हैं।
- सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएँ 43, 43ए, 66, 66बी, 66सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए और 74 हैकिंग और साइबर अपराधों से संबंधित हैं।
- सरकार ने साइबर सुरक्षा से संबंधित फ्रेमवर्क का अनुमोदन किया है और इसके लिये राष्ट्रीय सुरक्षा परिषद सचिवालय को नोडल एजेंसी बनाया गया है।
- राष्ट्रीय विशिष्ट अवसंरचना और विशिष्ट क्षेत्रों में साइबर सुरक्षा के लिये राष्ट्रीय प्रौद्योगिकी अनुसंधान संगठन को नोडल एजेंसी बनाया गया है।
- इसके अंतर्गत 2 वर्ष से लेकर उम्रकैद तथा दंड अथवा जुर्माने का भी प्रावधान है। सरकार द्वारा 'राष्ट्रीय साइबर सुरक्षा नीति, 2013' जारी की गई जिसके तहत सरकार ने अति-संवेदनशील सूचनाओं के संरक्षण के लिये 'राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure protection centre-NCIIPC) का गठन किया।
- सरकार द्वारा 'कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-In)' की स्थापना की गई जो कंप्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।
- विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने 'सूचना सुरक्षा शिक्षा और जागरूकता' (Information Security Education and Awareness: ISEA) परियोजना प्रारंभ की है।
- भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्य प्रणाली अपनाने के लिये अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है।
- अंतर-एजेंसी समन्वय के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Co-ordination Centre-I4C) की स्थापना की गई है।
- देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (Ministry of Electronics and Information Technology-MeitY) के तहत भारत सरकार की डिजिटल इंडिया मुहिम का एक हिस्सा है।

भारत इंटरनेट का तीसरा सबसे बड़ा उपयोगकर्त्ता है और हाल के वर्षों में साइबर अपराध कई गुना बढ़ गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिये सरकार की ओर से कई कदम उठाए गए हैं। कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी अतः भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा।

स्रोत: PIB

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/towards-a-new-national-cyber-security-strategy